Background Review

Read Appendix

Hao Zheng

Department of Computer Science and Engineering
University of South Florida
Tampa, FL 33620
Email: zheng@cse.usf.edu
Phone: (813)974-4757
Fax: (813)974-5456

Propositional Logic

Propositions

- A **logic statement** or **proposition** evaluates to true or false.
- Example: which of the following is a proposition?
  - Two plus two equals four
  - $2 + 3 = 4$
  - Tampa is south to Boston.
  - He is a college student
  - $x + y > 0$

Propositions

- **Compound propositions** can be constructed from simple ones with three symbols (**logic connectives**):
  - $\neg$: not; $\wedge$: and; $\vee$: or.
- Given two propositions p and q,
  - $\neg p$: the **negation** of p.
  - $p \wedge q$: the **conjunction** of p and q.
  - $p \vee q$: the **disjunction** of p and q.
- Order of operations: in an expression with $\neg$, $\wedge$ and $\vee$, $\neg$ applies first.
  - Use $()$ to avoid ambiguity in $p \wedge q \vee r$.

Logical Equivalence

Two propositions are called **logically equivalent** if, and only if, they have identical truth values for each possible truth assignment for their proposition variables. The logical equivalence of statements P and Q is denoted by writing $P \equiv Q$.

- Ex.: $p \wedge q \equiv q \wedge p$.

De Morgan's Law

- The negation of an **and** proposition is logically equivalent to the **or** proposition in which each component is negated.

$$\neg(p \wedge q) \equiv \neg p \vee \neg q$$

- The negation of an **or** proposition is logically equivalent to the **and** proposition in which each component is negated.

$$\neg(p \vee q) \equiv \neg p \wedge \neg q$$

Tautologies and Contradictions

- A proposition is a **tautology (valid)** if it is always true regardless of the truth values of the individual propositions substituted for its proposition variables. A tautology is denoted by **t**.

$$p \vee \neg p \equiv \mathbf{t}$$

- A proposition is a **contradiction** if it is always false regardless of the truth values of the individual propositions substituted for its proposition variables. A contradiction is denoted by **c**

$$p \wedge \neg p \equiv \mathbf{c}$$

- A proposition is **satisfiable** if there is at least one combination of values to the propositional variables that makes the formula be true. Ex.: $(a \vee b) \wedge c$
- Equivalences: $p \wedge \mathbf{t} \equiv p$, and $p \wedge \mathbf{c} \equiv \mathbf{c}$.
- What about $p \vee \mathbf{t} \equiv ?$, and $p \vee \mathbf{c} \equiv ?$

Conditional Propositions

- In a conditional proposition, a **conclusion** is derived from some hypotheses.

$$\text{If } \underbrace{4686 \text{ is divisible by } 6}_{hypothesis}, \text{ then } \underbrace{\text{it is divisible by } 3}_{conclusion}.$$

- If p and q are propositions, the **conditional** of q by p is "If p then q" or "p implies q" and is denoted $p \rightarrow q$.

p	q	$p \rightarrow q$
F	F	T
F	T	T
T	F	F
T	T	T

- p: **hypothesis** or **antecedent**
- q: **conclusion** or **consequent**

Vacuously True Conditional propositions

- Representing conditional propositions using OR

$$p \to q \ \equiv \ \neg p \vee q$$

.

- $p \to q$ is **vacuously true** if p is false.
- Example:

$$\text{if } 0 = 1, \text{ then } 1 = 2.$$

- **Order of operations**: $\neg$ applies first, $\wedge$, $\vee$ and $\oplus$ next, $\to$ applies the last.

Predicate Logic

Predicates

A **predicate** is a sentence that contains a finite number of variables and becomes a proposition when specific values are substituted for the variables.

The **domain** of a predicate variable is the set of all values that may be substituted in place of the variable.

Example:

- Let $P(x)$ be $x^2 > x$ where x is some real number where P is a predicate symbol.
- $P(x)$ becomes a proposition when a specific value is assigned to x.

Universal Quantifiers and Statements

- A predicate becomes a statements when all predicate variables are assigned with specific values.
    - Alternatively, use **quantifiers**.
- **Universal quantifier** $\forall$: "for all", "for each", "for any", "given any", etc
- Consider

$$\forall \text{ integer } x \in \mathbb{Z}, x > 0.$$

Think of x as an individual but generic object: an arbitrarily chosen integer.

Universal Quantifiers and Statements

- Let $Q(x)$ be a predicate and D the domain of x.
- A **universal statement** is a statement of the form "$\forall x \in D, Q(x)$, It is defined to be true if, and only if, $Q(x)$ is true for every x in D. It is defined to be false if, and only if, $Q(x)$ is false for at lease one x in D.

$$\forall x \in D, Q(x) \equiv Q(v_1) \wedge Q(v_2) \wedge \ldots$$

- A **counter-example** to a universal proposition is a value $x \in D$ such that $Q(x)$ is false.

Existential Quantifiers and Statements

Existential quantifier $\exists$: "there exists", "there is a", "for some", " there is at least one", etc.

- Let $Q(x)$ be a predicate and D the domain of x.
- An **existential** statement is a statement of the form "$\exists x \in D$ such that $Q(x)$". It is defined to be true if, and only if, $Q(x)$ is true for at lease one x in D. It is defined to be false if, and only if, $Q(x)$ is false for all x in D.

$$\exists x \in D, Q(x) \equiv Q(v_1) \vee Q(v_2) \vee \ldots$$

- A **witness** of an existential proposition is a value $x \in D$ such that $Q(x)$ is true.

Important Equivalences

$$
\begin{aligned}
\forall x.f(x) \circ g(y) &\equiv (\forall x.f(x)) \circ g(y) \\
\exists x.f(x) \circ g(y) &\equiv (\exists x.f(x)) \circ g(y) \\
\forall x.f(x) \wedge \forall x, g(x) &\equiv \forall x.(f(x) \wedge g(x)) \\
\exists x.f(x) \vee \exists x(x), g(x) &\equiv \exists x.(f(x) \vee g(x))
\end{aligned}
$$

Set Theory

Set Builder Notations

- A **set** is a collection of things called **elements** or **members**.
- Let S denote a set and let $P(x)$ be a property of the elements of S. We may define a new set to be the set of all elements x in S such that $P(x)$ is true. We denote this set as follows:

  $$\{x \in S \mid P(x)\}$$

  It reads as "the set of elements x such that $P(x)$ is true.
- Example:

  $$Z_1 = \{x \in \mathbb{Z} \mid x \geq 5\}$$

Subsets

- **Subsets** Given two sets A and B, A is called a **subset** of B, written $A \subseteq B$, if, and only if, every element of A is also an element of B.

$$A \subseteq B \quad \Leftrightarrow \quad \forall x, \text{ if } x \in A, \text{ then } x \in B.$$

The negation

$$A \nsubseteq B \quad \Leftrightarrow \quad \exists x \; st \; x \in A \wedge x \notin B.$$

- **Proper subsets** Given two sets A and B, A is a **proper subset** of B, written $A \subset B$, if and only if, every element of A is in B but there is at least one element of B that is not in A. Symbolically,

$$A \subset B \quad \Leftrightarrow \quad A \subseteq B \wedge B \nsubseteq A$$

Sets Equality

Given sets A and B, A **equals** B, written $A = B$, if and only if, every element of A is in B and every element of B is in A. Or symbolically,

$$A = B \quad \Leftrightarrow \quad A \subseteq B \text{ and } B \subseteq A$$

- Two sets are equal if they contain exactly the same elements.

Set Operations

- **Universal set** ($\mathbb{U}$): the set of all elements being considered in the context.
- **Intersection**: $A \cap B = \{x \in \mathbb{U} \mid x \in A \text{ and } x \in B\}$.
- **Union**: $A \cup B = \{x \in \mathbb{U} \mid x \in A \text{ or } x \in B\}$.
- **Difference**: $A - B = \{x \in \mathbb{U} \mid x \in A \text{ and } x \notin B\}$.
- **Complement**: $A^C = \{x \in \mathbb{U} \mid x \notin A\}$.

The Empty Set

- An **empty set** is a set with no elements, denoted $\emptyset$.
  - $\emptyset$ is a subset of every set.
  - There is only one empty set.
- Example: $\{1, 3\} \cap \{2, 4\}$ and $\{x \in \mathbb{R} \mid x^2 = -1\}$.

Partitions of Sets

$\{A_1, A_2, \ldots\}$ is a **partition** of A if, only if,

1. $A = A_1 \cup A_2 \cup \ldots$,
2. $A_1, A_2, \ldots$ are mutually disjoint.

- Example: Let $A = \{0, 1, 2, 3, 4, 5, 6, 7\}$, $A_1 = \{1, 3, 5\}$, $A_2 = \{2, 4, 6\}$ and $\{0, 7\}$. Is $\{A_1, A_2, A_3\}$ a partition of A?

Power Sets

- The **power set** of a set A, denoted $\mathcal{P}(A)$, is the set of all subsets of A. Also commonly written as

$$2^A$$

- Example: $A = \{1, 2, 3\}$.

Cartesian Products

- Given two sets A and B, the **Cartesian product** (also called **cross product**)) of A and B, denoted $A \times B$ (read "A cross B"), is the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$.

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$$

where (a, b) is called ordered pair.

Cartesian Products (cont'd)

- Given sets, $A_1, A_2, \ldots, A_n$, the **Cartesian product** of $A_1, A_2, \ldots, A_n$ denoted $A_1 \times A_2 \times \ldots \times A_n$ is the set of ordered n-tuples $(a_1, a_2, \ldots, a_n)$ where $a_1 \in A_1$, $a_2 \in A_2$, $\ldots$. Symbolically,

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots\}$$

- Example: $A_1 = A_2 = A3 = \{1, 2, 3\}$, find
  - $A_1 \times A_2 \times A_3$

Sets and Logic

- Recall the set builder notation

$$A = \{x \mid P(x)\} \text{ where } P \text{ is some predicate.}$$

  - $P(x)$ is also called the **characteristic** function of the set.
- This means that

$$x \in A \quad \Leftrightarrow \quad P(x) \text{ holds true.}$$

- Given a finite set, its characteristic function can be found by assigning an unique encoding to each element.
- Therefore, analyzing set relations can be done by logic analysis.
- Example: Let $A = \{x \mid P(x)\}$ and $B = \{x \mid Q(x)\}$. To check $A \subseteq B$, we can check if

$$\forall x,\, P(x) \rightarrow Q(x).$$

Sets and Logic

- Correspondence between set and logical operations

$$
\begin{array}{rcl}
A \cap B & \Leftrightarrow & P_A \wedge P_B \\
A \cup B & \Leftrightarrow & P_A \vee P_B \\
A - B & \Leftrightarrow & P_A \wedge \neg P_B \\
A \subseteq B & \Leftrightarrow & P_A \rightarrow P_B
\end{array}
$$

where P_A and P_B are predicates defining sets A and B.

Relations

Definition

Let A and B be sets. A (binary) **relation** R from A to B is a subset of $A \times B$. Give an ordered pair (x, y) in $A \times B$, x is related to y by R, written xRy, if, and only if, $(x, y) \in R$. A is the domain and B is the co-domain of R.

- Let $A = \{1, 2, 4\}$ and $B = \{1, 2, 3\}$ and define relation S from A to B as follows:

$$\forall (x, y) \in A \times B, (x, y) \in S \;\Leftrightarrow\; x < y$$

Properties of Relations

- Let R be a binary relation on a set A.
- R is **reflexive** if and only if, for all $x \in A$,

$$xRx$$

- R is **symmetric** if and only if, for all $x, y \in A$,

$$xRy \;\Rightarrow\; yRx.$$

- R is **anti-symmetric**, if and only if, for all $x, y \in A$,

$$xRy \wedge yRx \;\Rightarrow\; x = y.$$

- R is **transitive**, if and only if, for all $x, y, z \in A$,

$$xRy \wedge yRz \;\Rightarrow\; xRz.$$

Relations on Infinite Sets

- A relation R is defined as

$$\forall (x, y) \in \mathbb{R} \times \mathbb{R},\ xRy \ \Leftrightarrow x = y$$

Is R reflexive, symmetric, anti-symmetric, transitive?

Relations on Infinite Sets

- A relation S is defined as

$$\forall (x, y) \in \mathbb{R} \times \mathbb{R},\ xSy \ \Leftrightarrow x \leq y$$

Is S reflexive, symmetric, anti-symmetric, transitive?

Formal Languages

Words over an Alphabet

- An **alphabet** Σ is a set of symbols.
- A **word** over Σ is a finite or infinite sequence of symbols from Σ

$$w = A_0 A_1 \ldots A_n \text{ or } w = A_0 A_1 \ldots \text{ or } w = \epsilon.$$

- Σ^*: all finite words over Σ.
  - $\Sigma^+ = \Sigma^* - \{\epsilon\}$.
- Σ^ω: all infinite words over Σ.
- A **language** over Σ is the set of finite or infinite words over Σ.
- A **prefix** of $w = A_0 A_1 \ldots A_n$ is $w = A_0 \ldots A_i$ $(i \leq n)$.
  - Similarly defined for infinite words.
- A **suffix** of $w = A_0 A_1 \ldots A_n$ is $w = A_i \ldots A_n$ $(i \geq 0)$.
  - No suffix is defined for infinite words.

Operations on Words and Languages

- **Concatenation**
  - $BA \cdot AAB = BAAAB$.
- **Repetition** of a word: $(AB)^2 = ABAB$.
  - Special cases: $w^0 = \epsilon$, $w^1 = w$.
- Finite repetition of finite words using *Kleene star* $*$.
  - w^* is a language including words that are finite number of repetitions of w.
  - Ex: $(AB)^* = \{\epsilon, AB, ABAB, ABABAB, \ldots\}$.
- Concatenation and repetition are defined similarly for languages.

Regular Languages

- A **regular expression** over Σ is defined recursively by
  - $\emptyset$ and ϵ are regular expressions.
  - A is a regular expression for every $A \in \Sigma$.
  - If E_1, E_2, and E are regular expressions, so are $E_1 + E_2$, $E_1 \cdot E_2$ and E^*
- A language is **regular** if every word of the language is represented by a regular expression.
  - The language induced by a regular expression E is $\mathcal{L}(E)$, and
  - $\mathcal{L}(\emptyset) = \emptyset$, $\mathcal{L}(\epsilon) = \{\epsilon\}$, $\mathcal{L}(A) = \{A\}$, and
  - $\mathcal{L}(E_1 + E_2) = \mathcal{L}(E_1) \cup \mathcal{L}(E_2)$, $\mathcal{L}(E_1 \cdot E_2) = \mathcal{L}(E_1) \cdot \mathcal{L}(E_2)$, $\mathcal{L}(E_1 + E_2) = \mathcal{L}(E^*) \cup (\mathcal{L}(E))^*$.
- A regular language can also be represented by a automata.